BY ORDER OF THE COMMANDER
AIR FORCE SPACE COMMAND

AIR FORCE INSTRUCTION 10-1701

AIR FORCE SPACE COMMAND
Supplement

10 JANUARY 2018

Operations

COMMAND AND CONTROL (C2) FOR CYBERSPACE OPERATIONS

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: Publications and forms are available on the e-Publishing website at **www.e-Publishing.af.mil** for downloading or ordering

RELEASABILITY: There are no releasability restrictions on this publication

---

OPR: HQ AFSPC/A2/3/6W

Certified by: HQ AFSPC/A2/3/6W
(Colonel Lorinda A. Frederick)

Pages: 6

This supplement implements and extends the guidance of AFI 10-1701, *Command and Control (C2) for Cyberspace Operations.* This supplement describes the Air Force Space Command (AFSPC) procedures for use in conjunction with the basic AFI. It applies to HQ AFSPC, subordinate Numbered Air Forces (NAFs) and subordinate units. It applies to the Air National Guard and the Air Force Reserve AFSPC gained units and members under U.S.C. Title 10 status, upon mobilization. The authorities to waive wing/unit level requirements in this publication are identified with a Tier ("T-0, T-1, T-2, T-3") number following the compliance statement. See AFI 33-360, *Publications and Forms Management*, Table 1.1 for a description of the authorities associated with the Tier numbers. This AFI may be supplemented at any level, but all supplements must be routed to OPR for coordination prior to certification and approval. Refer recommended changes and questions about this publication to the Office of Primary Responsibility (OPR) using the AF Form 847, *Recommendation for Change of Publication*; route AF Forms 847 from the field through appropriate functional's chain of command. Ensure that all records created as a result of processes prescribed in this publication are maintained IAW Air Force Manual (AFMAN) 33-363, Management of Records, and disposed of IAW Air Force Records Information Management System (AFRIMS) Records Disposition Schedule (RDS).

SUMMARY OF CHANGES

This is a new supplement and must be completely reviewed.

1.1. In accordance with AFSPC OPORD 17-01, 24 AF/CC is delegated authority to ensure the Service portion of the DODIN (AFIN) is secure, assured, and interoperable, and that all personnel are appropriately trained. USCYBERCOM delegated authority for cyberspace operations over all Department of the Air Force components to CDR AFCYBER to effectively implement orders from USCYBERCOM/JFHQ-DODIN and to ensure the timely and efficient security, operation, and defense of the Air Force portion of the DODIN. Cyber orders issued by 24 AF/CC are military orders; AFSPC units developing systems to operate or already operating within the AFIN will take appropriate actions to comply with 24 AF orders to secure and defend the AFIN, and direct cyberspace operations as required in support of requesting CCDRs. Appropriate actions regarding orders which impact mission systems should reflect the Commander's assessment of primary mission risk and exigency, as well as fleet configuration responsibilities of the PMO. If compliance is deemed impossible or impracticable, communicate this fact, with full explanation, to 614 AOC and 624 OC IAW paragraphs 2.5.1, and 2.5.6.2.

1.2. AFSPC units developing systems to operate or already operating within the DoDIN will take appropriate actions to comply with AFCYBER orders to operate and defend the AFIN and direct cyberspace operations as required in support of requesting CCDRs.

1.3. The AF identified cyberspace threats to mission systems as a critical concern. Effective cyber C2 in support of AFSPC space operations requires a common activity framework that enables unity of effort with 24 AF, 14 AF, operational wings, Space and Missile Systems Center (SMC) program offices, and the Air Force Life Cycle Management Center (AFLCMC). Protecting a mission/weapon systems from cyberspace threat is a collaborative effort across several organizations. The intent is to assure Joint Force Commanders (JFC) mission/weapon systems upon which they depend will operate as intended at the time and place of their choosing.

1.3.1. An "EXORD to Implement Updated Cyberspace Operations Command and Control", was issued 01 Feb 16. It does not limit the authority of the Air Force to proactively strengthen networks or to take actions internally to defend them. Such activity should be consistent with applicable cyber orders.

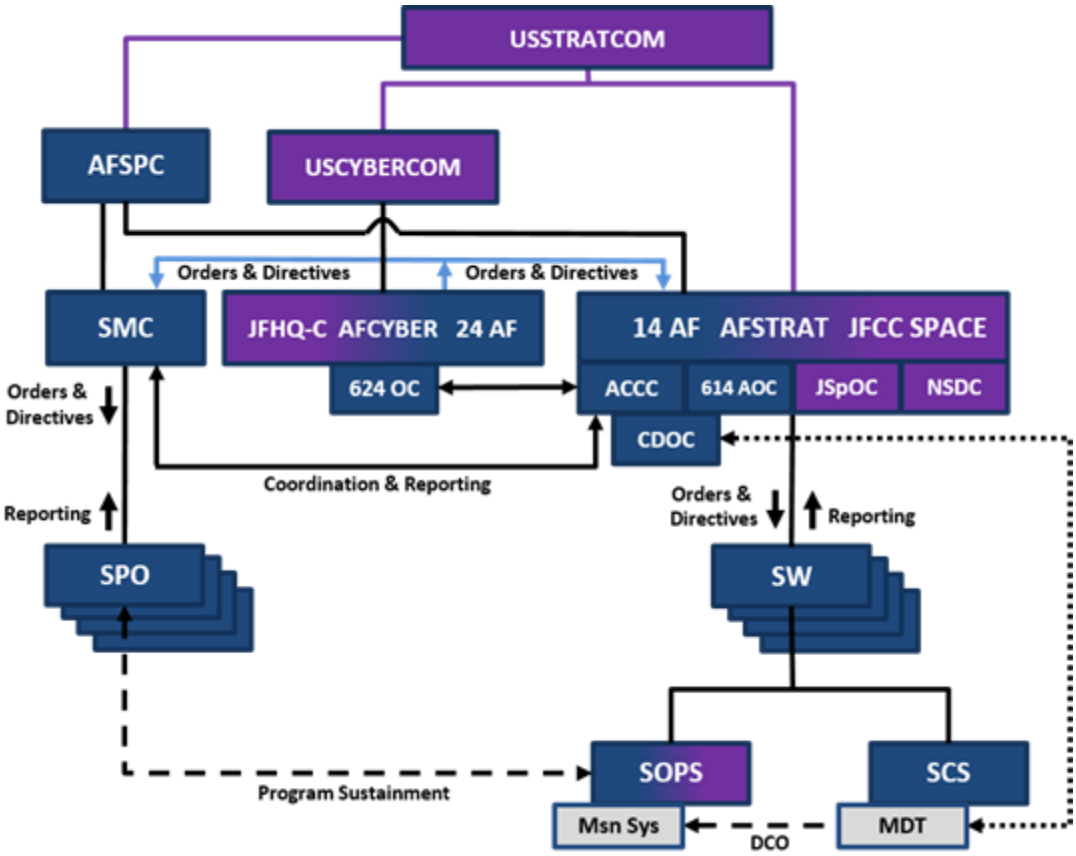
1.4.1. Commanders of units assigned/attached to AFSPC shall ensure compliance with orders issued pursuant to this instruction and hold personnel and organizations accountable for the consequences of non-compliance. **(T-2)**.

1.4.1.1. AFSPC assigned military personnel and civilian employees may be subject to administrative and/or judicial actions if they knowingly, willfully, or negligently compromise, damage, or place at risk information and information systems by failure to comply with cyber orders issued by 24 AF/AFCYBER.

1.6. AFSPC Cyber Orders Flow Process. Figure 2 graphically depicts the flow of cyber orders.

1.6.1. Cyber Orders Distribution. Applicable cyber orders are distributed by the 624 OC to 14 AF and SMC for actions affecting assets not under the direct control or ownership of 24 AF.

Figure 2. (Added) The AFSPC Cyber Orders Flow Process.



2.3. 614th Air and Space Operations Center (614 AOC). The 614 AOC is the 14 AF operations center responsible for the C2 of assigned and attached forces that focus on global and theater space operations. The 614 AOC will maintain awareness of weapon system cyber health and status via coordination with 14 AF ACCC and 14 AF Director of Cyberspace Forces (DIRCYBERFOR).

2.3.1. The AF-wide tasking system for AF cyber orders does not account specifically for space core function lead mission/weapon systems. 14 AF will develop/utilize a supplemental AFSPC-wide tasking system for AF cyber orders. 14 AF ACCC will relay receipt and status to 624 OC on a continuous basis. (**T-2**).

2.5. 14 AF ACCC, SMC, DIRCYBERFOR, 14 AF Cyber Defense Operations Center (CDOC) (when fielded).

2.5.1. AFSPC commanders or their designated representatives may request relief from cyber orders due to operational impacts via 24 AF/AFCYBER-defined orders relief processes. Relief request from 14 AF units will be processed through wing command channels to the 14 AF ACCC. The 14 ACCC will coordinate the request through the 624 OC and forward to 24 AF for determination. Relief from cyber orders shall be reflected in the overall cyber resiliency of the system.

2.5.4. The 14 AF ACCC will:

2.5.4.1. Task and delegate space wings under its purview and SMC with cyber orders from superior authorities such as USSTRATCOM, AFSPC, USCYBERCOM, and AFCYBER.

2.5.4.4. 14 AF ACCC will inform space and cyber mission system commanders and DIRCYBERFOR on the operational impacts of cyber orders to space mission systems and component missions.

2.5.4.8. **(Added)** Establish process to receive, track, report, and take action on cyber orders.

2.5.4.9. **(Added)** Take input on cyber threats and consider intelligence given in the overall space situational awareness posture.

2.5.4.10. **(Added)** Prioritize and coordinate 24 AF Requests for Service/Support received by all 14 AF wings through 24 AF processes.

2.5.6. SMC will establish a single entry point and processes to receive, process, track and action cyber orders from 24 AF/AFCYBER and 14 AF ACCC. SMC will respond to and report cyber order/tasking status back through 14 AF ACCC. SMC will ensure new space capabilities are fielded with cybersecurity resiliency as a mandatory component of the acquisition process; where feasible, retrofit cybersecurity capabilities into fielded space mission systems; and develop emergency response processes to address critical cyber threats and vulnerabilities to space mission systems for which SMC is responsible.

2.5.6.2. Relief from cyber order requests will be processed through wing command channels to the 14 AF ACCC. The 14 AF ACCC will coordinate the request through the 624 OC and forward to 24 AF for determination.

2.5.6.6. SMC will provide a SITREP to the 14 AF ACCC related to any space mission system outage impacting the AFSPC mission.

2.5.7. **(Added)** 14 AF DIRCYBERFOR is the senior 14 AF Air Force Cyberspace Operations Officer and serves as the principal advisor to the 14 AF/CC for cyberspace operations. The DIRCYBERFOR will advise the 14 AF CDOC and will advocate for and assist in the coordination of other cyber forces as required. To ensure close coordination with the overall effort, the DIRCYBERFOR establishes Direct Liaison Authorized (DIRLAUTH) with AFCYBER, United States Cyber Command (USCYBERCOM) via the USSTRATCOM Joint Cyberspace Center (JCC), and other elements of the joint cyberspace community as required. The DIRCYBERFOR coordinates with the 14 AF staff to fully integrate cyberspace operational capabilities into the planning cycle. The DIRCYBERFOR facilitates coordination, planning, execution, and assessment of Air Force cyber operations for 14 AF/CC.

2.5.7.1. **(Added)** The DIRCYBERFOR will advise the 14 AF CDOC in their mission to protect, monitor, detect, analyze, and respond to cyber incidents on or against space mission systems. The DIRCYBERFOR will advocate for and assist in the coordination of other AFCYBER weapon system support as required.

2.5.8. **(Added)** The 14 AF CDOC (when fielded) is charged with protecting, monitoring, detecting, analyzing and responding to all cyber events on or against any Air Force space mission system. The CDOC will integrate cyber security defense with wing Defensive Cyberspace Operations (DCO) resources in a tiered incident response capability. The 14 AF CDOC will collaborate with 14 AF ACCC, SMC, and the mission owner for information sharing and incident response efforts. The CDOC will employ cybersecurity tools and technologies for monitoring, detecting, analyzing and responding to cybersecurity events. The CDOC will operate 24X7X365 to provide continuous response capabilities including incident categorization, prioritization, escalation/de-escalation, and response management.

4.3. 14 AF units will report PONDs through 14 AF ACCC.

JOSEPH T. GUASTELLA JR., Major General, USAF
Director of Air, Space,
Cyberspace and ISR Operations

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

Abbreviations and Acronyms

614 AOC - 614th Air and Space Operations Center

AFLCMC - Air Force Life Cycle Management Center

CDOC - Cyber Defense Operations Center

DCO – Defensive Cyberspace Operations

DIRCYBERFOR - Director of Cyberspace Forces

DIRLAUTH - Direct Liaison Authorized

JCC - Joint Cyberspace Center

SMC - Space and Missile Systems Center